UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

TIMOTHY LIVINGSTON, **Petitioner,** **v.** **UNITED STATES,** **Respondent.**	19-cv-12656 **OPINION**

WILLIAM J. MARTINI, U.S.D.J.:

This matter arises out of Timothy Livingston's ("Petitioner") petition for habeas corpus relief under 28 U.S.C. § 2255. On November 18, 2019, this Court rejected the petition as procedurally barred. ECF No. 8. The matter comes before the Court on Petitioner's motion for reconsideration pursuant to FRCP 59. ECF No. 10. For the reasons set forth below, the motion is **DENIED**.

I. BACKGROUND

The facts and procedural history of this matter were set forth in the Court's November 19, 2019 Opinion ("November Opinion"), familiarity with which is assumed. ECF No. 8. In short, the November Opinion denied the Petition as time barred. *Id.* Since the November Opinion, Petitioner moved for reconsideration, then appealed. ECF Nos. 10, 13-14.[1] After reviewing the briefing, the Court ordered the Government to file a sur-reply specifically addressing issues raised in Petitioner's reply brief. ECF No. 18. After delays caused by the Corona Virus outbreak, the Government filed its sur-reply on May 18, 2020. ECF No. 26. Due to technical difficulties, exhibits followed. ECF Nos. 27 & 29. The Court also permitted Petitioner to respond to the Government's submissions. ECF Nos. 32-33.

II. DISCUSSION

Petitioner moves for reconsideration of the Court's November Opinion and associated Order, ECF No. 9. Petitioner argues his petition is reviewable because (1) he is actually innocent (excusing untimeliness) and (2) the Government improperly withheld evidence (tolling the time period). Mot. at 1.

---

[1] Despite the appeal, this Court retains jurisdiction over the motion for reconsideration. *See United Nat. Ins. Co. v. R & D Latex Corp.*, 242 F.3d 1102, 1109 (9th Cir. 2001) (citing Fed. R. App. P. 4(a)(4)(B)(i)).

A. Motion for Reconsideration Standard

Decisions may be altered or amended by a motion for reconsideration "if the party seeking reconsideration shows at least one of the following grounds: (1) an intervening change in the controlling law; (2) the availability of new evidence that was not available when the court granted the [prior motion]; or (3) the need to correct a clear error of law or fact or to prevent manifest injustice." *Howard Hess Dental Labs., Inc. v. Dentsply Int'l Inc.*, 602 F.3d 237, 251 (3d Cir.2010). Petitioner has not pointed to any fact or law justifying reconsideration of the November Opinion.

B. No Hearing is Necessary and no Error Occurred

"[B]ald assertions and conclusory allegations do not afford a sufficient ground for an evidentiary hearing on a habeas petition." *See Palmer v. Hendricks*, 592 F.3d 386, 395 (3d Cir. 2010) (citation omitted). "[E]ven if the factual allegations in the habeas petition are sufficient to make out a prima facie claim for habeas relief, a district court may decline to convene an evidentiary hearing if the factual allegations are contravened by the existing record." *Id.* at 393. Here, to the extent Petitioner's arguments go beyond conclusory accusations of prosecutorial misconduct, they are contradicted by the record.[2]

1. Improper Withholding of Evidence

Petitioner argues (1) the Government failed "to provide requested exculpatory evidence necessary to the successful litigation of his 2255 Motion"; (2) "[d]uring the criminal proceedings Counsel failed to obtain exculpatory evidence"; (3) and "the Government has failed to provide the *Brady* evidence necessary to properly support the arguments raised in" Petitioner's original motion. Mot. at 3. Petitioner also notes certain FOIA requests he made and his post-conviction counsel, apparently hired "to obtain copies of the digital evidence." *Id.* Petitioner is thin on specifics, but notes "nearly all" the relevant evidence exists on his personal hard drives, of which the Government has failed to provide copies. *Id.* Thus, Petitioner argues, his petition was timely and the November Opinion incorrect. *Id.*

The Government responds that copies of the hard drives were "available to the Petitioner months in advance of his plea." Opp. at 4, ECF No. 16. In reply, Petitioner quotes a letter from his trial counsel, noting that she had "not yet been able to personally review each and every page of exhibit thus far disclosed by the government" and "Defendant has never seen and has no knowledge concerning the overwhelming majority of exhibits provided in discovery." Reply at 4 (quoting Ex. 1), ECF No. 17. Contrary to Petitioner's belief that his Counsel's letter shows the evidence was improperly withheld, it actually demonstrates the opposite. Petitioner's trial counsel received digital copies of the

---

[2] Petitioner's final submission contains various accusations of illegal conduct by other individuals. Whether others acted illegally is not dispositive to the question of whether Petitioner is actually innocent. As discussed below, he is not. Further, the fact that Petitioner had legitimate clients or the software he utilized has legal uses does not remedy the illegal manner in which he did business.

evidence. She may not have reviewed them before sending the letter, but nothing indicates Petitioner could not have reviewed them himself, either before the plea or before the time limit for filing Section 2255 motions.

Petitioner's allegations regarding the Government's failure to turn over hard drives to his post-conviction counsel do not justify relief or require a hearing either. First, as noted, the record cited by Petitioner shows his trial counsel had copies of the evidence. *Id.* Second, Petitioner filed the present petition despite the Government's alleged *continuing* violation. Thus, the Government was not an impediment and the relevant facts were already known (or readily available) more than a year before Petitioner filed for habeas relief. *See* 28 U.S.C. § 2255(f) (extending limitations period one year after government's impediment removed or facts could have been discovered through exercise of due diligence). Third, as will be discussed below, the record definitively shows that the hard drives do not contain what Petitioner claims—proof of his actual innocence. *See Palmer*, 592 F.3d at 395 (finding hearing non-mandatory "if the factual allegations are contravened by the existing record."). Accordingly, the alleged failure to turn over exculpable evidence does not mandate a hearing or justify reconsideration of the Court's decision on timeliness.[3]

2. The Record Refutes Petitioner's Claims of Actual Innocence

Petitioner argues his actual innocence requires the Court to reconsider the November Opinion and hear his late Section 2255 petition. While Petitioner's arguments could have been—and in many cases, were—raised in the original motion (and thus do not support reconsideration), given Petitioner's *pro se* status and to protect against "manifest injustice," the Court will address each count.

a. Count One

Petitioner argues he is factually innocent because (1) "spam is legal" and (2) his conduct does not amount to criminal conspiracy. Mot. at 4-8. First, Petitioner was prosecuted for the particular (and illegal) way he went about sending spam, not the mere act of spamming. Second, the record demonstrates a criminal conspiracy existed. Even setting aside Petitioner's own admissions, ECF No. 27-2 (admitting guilt), Petitioner's co-conspirator admitted to the charged conduct. *See* ECF No. 27-7 (cooperator plea). Records of Petitioner's online conversations show he worked with his co-conspirator to test and improve a computer program specifically designed to access and manipulate others' email accounts. ECF No. 27-10. They discussed payment, including as a percentage of Petitioner's profits. *See id.* And Petitioner's co-conspirator did, in fact, share the computer program with Petitioner. *See* ECF No. 27-4 (analysis of data stored on Petitioner's

---

[3] The Court appreciates the Government's efforts to contact Petitioner's post-conviction counsel to inquire about the matter. Sur Reply at 13. While counsel's representations do not form the basis of the Court's opinion, the Government appears to have seriously inquired if it improperly withheld evidence.

website). In other words, they reached an agreement to violate the underlying statutes and took overt steps toward that goal.

The remainder of Petitioner's arguments are essentially that his conduct does not satisfy the elements of the underlying offences. That is incorrect. The Court already addressed the loss threshold issue and will not do so again here. *See* November Opinion (explaining that $5,000 in losses was not a necessary element of the conspiracy count). With respect to Petitioner's remaining arguments, the Government would have only needed to prove a conspiracy to commit one of the underlying offenses. *See* 3d Cir. Model Jury Instruction 6.18.371A. Petitioner's conclusory assertions aside, the record clearly demonstrates Petitioner conspired to violate 18 U.S.C. § 1030(a)(5)(A).

Section 1030(a)(5)(A) prohibits individuals from "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." "[T]he term 'protected computer' means a computer . . . which is used in . . . interstate or foreign . . . communication." 18 U.S.C. § 1030(e). "Damage" includes "any impairment to the integrity or availability of data." *Id.* Here, by working with his co-conspirator to test and improve a program that manipulates users' email accounts to send spam—including a "clear folders" function, ECF No. 27-10—Petitioner conspired to impair the "availability of data," 18 U.S.C. § 1030(e).[4] The contents of the accounts were held on "protected computers," i.e., the corporate victim's servers, which are used in interstate communication. *Id.* Thus, Petitioner conspired to violate 18 U.S.C. § 1030(a)(5)(A), in violation of 18 U.S.C. § 371.

b. Count Two

Count Two charged plaintiff with conspiracy to commit fraud and related activity in connection with electronic mail, in violation of several subsections of 18 U.S.C. § 1037(a). Section 1037(a)(1) prohibits individuals from knowingly "accesses[ing] a protected computer without authorization, and intentionally initiat[ing] the transmission of multiple commercial electronic mail messages from or through such computer," or conspiring to do so. Here, Petitioner collaborated with another individual to test a computer program aimed at using accounts held on the Corporate Victim's servers, in order to send spam from those accounts, without authorization. ECF No. 27-10 (skype conversation demonstrating testing of computer program); ECF No. 27-4 (analysis of website contents, including computer program at issue). Accordingly, Petitioner conspired to commit fraud in connection with electronic mail.

---

[4] Petitioner argues having such a function is normal, but in his skype chat, Petitioner's co-conspirator stated "when you start doing real #s . . . you need that," to which Petitioner responded "oh alright." ECF No. 27-10. Thus, the co-conspirators agreed to use the computer program, including the clear folders function, to damage protected computers. Much like a knife—which has both legal and illegal uses—it was not the program itself that made Petitioner's conduct illegal, it was the way Petitioner schemed with another to use it.

c. Count Six

Petitioner also plead guilty to Count Six, aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(1). Section 1028A(a)(1) dictates that "[w]hoever, during and in relation to any [violation of 18 U.S.C. §§ 1030 or 1037)], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years." "[T]he term 'means of identification' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." 18 U.S.C. § 1028. The term includes any "name, social security number, date of birth, official State or government issued driver's license or identification number, . . . unique electronic identification number, address, or routing code." *Id.*; *see also United States v. Kvashuk*, 443 F. Supp. 3d 1263, 1268 (W.D. Wash. 2020) ("Use of usernames and passwords that identify specific individuals can constitute a means of identification.")

Here, Defendant maintained a vast database of stolen identification information to execute his spamming scheme, including email addresses, usernames, and passwords. ECF No. 27-4 (analysis of data stored on Petitioner's website). Petitioner's skype conversations confirm he knowingly used his access to others' "means of identification" to spam email accounts. *See* ECF No. 27-11 (skype conversation confirming Petitioner did "internal mailing" and sent out one million emails per day using corporate victim accounts).[5]

III. CONCLUSION

The Court need not address the remainder of Defendant's specific sub-arguments, which are either repudiated by the above or the Court's November Opinion, conclusory, contrary to the record, or unsupported by applicable law. Accordingly, Petitioner's motion for reconsideration, ECF No. 10, is **DENIED**. An appropriate order follows.

Date: September 14, 2020

WILLIAM J. MARTINI, U.S.D.J.

[5] Petitioner argues that some unknown individual, or the FBI itself, planted files on his website and created fake skype chat logs. ECF No. 33 at 18. The Court does not credit this new allegation, nor other bald, fresh allegations of misconduct. The Government was clear in its position that Defendant maintained the website storing millions of illegally obtained access credentials since its initial opposition brief. *See* Opp. at 2, ECF No. 6. Petitioner cannot wait until a sur-sur reply on a motion for reconsideration to try to undermine that inconvenient fact.